Remarks

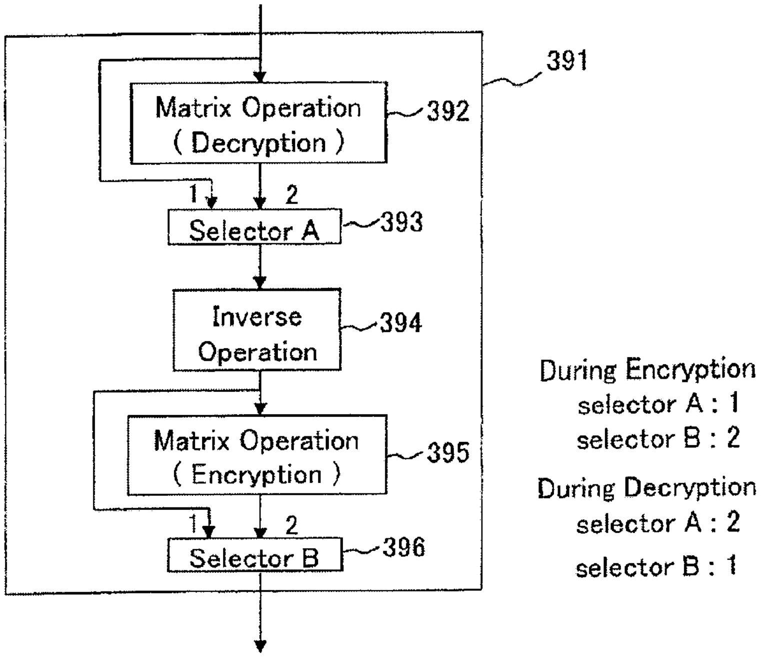
In the non-final Office Action dated January 15, 2010, the following new grounds of rejection are presented: claims 1-2, 4-5, 8-10, 12-15 and 18-19 stand rejected under 35 U.S.C. § 103(a) over Van Buer (U.S. Patent Pub. 2003/0198345) in view of Okada (U.S. Patent Pub. No. 2003/0108195); and claims 6-7, 11 and 16-17 stand rejected under 35 U.S.C. § 103(a) over the '345 and '195 references in view of Dent (U.S. Patent No. 5,091,942). Claim 3 is objected to as being dependent upon a rejected base claim but would be allowable if rewritten in independent form. Applicant addresses these rejections in the following discussion which does not acquiesce in any regard to averments in this Office Action (unless Applicant expressly indicates otherwise).

Applicant appreciates the indicated allowability of claim 3, if written in independent form.

The cited portions of the references do not appear to be relevant to aspects of the claim limitations. In an effort to assist the Examiner's review and to facilitate prosecution, Applicant presents the following technical discussion of embodiments described in Applicant's specification. Applicant's specification explains that a load pattern is the first row of each matrix. (*See, e.g.*, Applicant's specification, p. 5 "In the present invention, the first row of each matrix is termed the 'load pattern.'") Applicant's specification also teaches a single all-affine transformation that performs both affine and inverse affine transformations depending upon the load pattern (the first row of each matrix). (*See, e.g.*, Applicant's specification, p. 5 "Each occurrence in the AES/Rinjndael of the pair of affine transform and inverse affine transform is reduced by the present invention to one transform, the Affine-All transform.") Applicant's specification teaches embodiments in which a single Affine-All transform performs both affine and inverse affine functions based upon the first row of each matrix or the load pattern. It should be clear that the two separate matrix operations, implemented by two different logic circuits would not correspond to an Affine-All transform that performs both affine and inverse affine functions based upon a load pattern.

Applicant respectfully traverses the § 103(a) rejections of claims 1-2 and 4-19 because the cited '345 reference either alone or in combination with the '195 reference lacks correspondence to the claimed invention. Moreover, the addition of the '942 reference does not cure the underlying lack of correspondence. While the relied upon portion of the secondary '195 reference suggests some circuitry can be shared, the secondary '195 reference does not teach or suggest correspondence to claim limitations directed toward one affine-all transformation that performs both an affine transformation and an inverse affine transformation, the particulars of which can be in response to a load pattern.

The cited paragraph 186 of the secondary '195 reference appears to be referencing implementations that relate to FIG. 10 (reproduced below). FIG. 10 and the accompanying description teach the use of two different matrix operations (392 and 395). The first matrix operation is implemented for decryption and the second matrix operation is implemented for encryption. The specifics of each of these operations are taught to be implemented using two different circuits (*e.g.*, either the circuits of FIGs. 11-12 or the circuits of FIGs. 13-14). As each of these matrix operations are implemented using different circuits and different transforms, Applicant submits that the Office Action has not shown correspondence to the claim limitations that are directed towards an affine-all transformation that performs both an affine and inverse affine transformation, which can be in response to respective load patterns. For at least these reasons, the proposed modification does not correspond to the claim limitations as a whole.



In view of the remarks above, Applicant believes that each of the rejections has been overcome and the application is in condition for allowance. Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the agent overseeing the application file, Juergen Krause-Polstorff, of NXP Corporation at (408) 474-9062 (or the undersigned).

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131

CUSTOMER NO. 65913

By: ______________________
Robert J. Crawford
Reg. No.: 32,122
Shane O. Sondreal
Reg. No.: 60,145
651-686-6633
(NXPS.604PA)